X.509 Certificate Policy

for the

Government Printing Office

Certification Authority

(GPO-CA)

August 17, 2009

Version 1.3.1

FOR OFFICIAL USE ONLY

SIGNATURE PAGE

_____ _____

Chair, Government Printing Office Public Key Infrastructure Steering Committee DATE

_____ _____

Chair, Government Printing Office Public Key Infrastructure Policy Authority DATE

_____ _____

Government Printing Office Public Key Infrastructure Operational Authority DATE

TABLE OF CONTENTS

RECORD OF CHANGES

Version	Date	Author(s)	Reason	Description
1.0	8 September 2003	CygnaCom Solutions, Inc	Initial Document	Initial Document
1.0.1	1 October 2004	CygnaCom Solutions, Inc	Minor changes for FBCA CP mapping for FBCA cross certification	Address the four comments from the FBCA CP mapping
1.1	27 February 2006	U.S. Government Printing Office	Changes to comply with Federal PKI Common Policy and PKI Shared Service Provider (SSP) requirements	Changes in various sections to comply with Federal PKI Common Policy and PKI Shared Service Provider (SSP) requirements
1.2	1 July 2006	U.S. Government Printing Office	Changes to comply with AICPAWebTrust for CA audit requirements	Changes in various sections to comply with the AICPA WebTrust for CA audit requirements, as recommended by WebTrust auditor and GPO OIG recommendations.

Version	Date	Author(s)	Reason	Description
1.3	March 14, 2009	U. S. Government Printing Office	Changes to format the CP to the RFC 3647 requirements, to include GPO specific policy requirements for GPO Medium-Hardware Assurance, GPO Authentication and GPO CardAuth certificates, and general compliance with the Federal PKI FBCA CP and Common Policy.	Changes to various sections to address GPO specific policy requirements for GPO Medium-Hardware Assurance, GPO Authentication and GPO CardAuth certificates, for RFC 3647 format, and for general compliance with the Federal PKI Common Policy and FBCA CP.
1.3.1	August 17, 2009	U.S. Government Printing Office	Minor updates to respond to Federal PKI Certificate Policy Working Group (CPWG) comments.	Changes to certain sections to address CPWG comments.

1. INTRODUCTION

This Certificate Policy (CP) defines the certificate policy for use by the Government Printing Office Certification Authority (GPO-CA) to facilitate interoperability between other PKI Domains and CAs External to the GPO-CA. This policy represents Medium Assurance and , Medium-Hardware Assurance Levels for public key digital certificates. In addition, this policy includes certificate types for Device certificates, Authentication certificates and CardAuth certificates. The word "assurance" used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. In addition, it also reflects how well the Relying Party can be certain that the individual whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate, and how securely the system which was used to produce the certificate and (if appropriate) deliver the private key to the subscriber performs its task.

This GPO CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Certificate Policy and Certification Practices Statement Framework.

The terms and provisions of this GPO CP shall be interpreted under and governed by applicable Federal law.

1.1 OVERVIEW

1.1.1 Certificate Policy (CP)

GPO-CA certificates contain a registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The party that registers the OID (in this case, the U.S. Government GPO) also publishes the CP, for examination by Relying Parties. Each CA certificate issued by the GPO-CA will, in the *policyMappings* extension and in whatever other fashion is determined by the GPO-CA to be necessary for interoperability, reflect what mappings the GPO PKI Policy Authority determines shall exist between the GPO CP and the Entity CP.

1.1.2 Relationship Between the GPO CP and CPS

The GPO CP states what assurance can be placed in a certificate issued by the GPO-CA. The GPO CPS states how the GPO-CA establishes that assurance.

1.1.3 Scope

The GPO-CA exists to facilitate trusted electronic business transactions for the GPO and federal organizations. To facilitate the missions of the GPO and federal organizations, interoperability is offered to non-federal entities in accordance with federal PKI requirements, federal law and GPO

business processes. The interoperability information in this CP applies equally to federal organizations and other organizations owning or operating PKI domains. As used in this CP, Entity PKI or Entity CA may refer to an organization's PKI, a PKI provided by a commercial service, or a bridge CA serving a community of interest.

1.1.4 Interoperation with CAs Issuing under Different Policies

This CP provides for interoperability with Entity CAs (CAs external to the GPO, non-GPO-CAs) through cross certification. Interoperability will be established when directed by the GPO-PA and will require a Memorandum of Agreement (MOA), between the GPO-CA and the Entity CA, and may require changes to this CP to address issues associated with liability and other matters. In particular, interoperation with the Federal PKI Common Policy Framework and the Federal Bridge CA are facilitated by this CP.

1.2 DOCUMENT NAME AND IDENTIFICATION

The Medium Assurance and Medium-Hardware Assurance levels are defined in subsequent sections of this CP. The GPO Medium Assurance and Medium-Hardware Assurance levels, along with Authentication, Device and CardAuth certificates, have corresponding Object Identifiers (OIDs), to be asserted in certificates issued by the GPO-CA, which comply with the policy stipulations herein. The OIDs are registered under the id-infosec arc as follows:

csor-certpolicy ::= {2 16 840 1 101 3 2 1}

id-gpo-policies ::= {csor-certpolicy 17}

id-gpo-certpcy-mediumAssurance	::= {2 16 840 1 101 3 2 1 17 1}
id-gpo-certpcy-mediumHardware	::= {2 16 840 1 101 3 2 1 17 2}
id-gpo-certpcy-devices	::= {2 16 840 1 101 3 2 1 17 3}
id-gpo-certpcy-authentication	::= {2 16 840 1 101 3 2 1 17 4}
id-gpo-certpcy-cardAuth	::= {2 16 840 1 101 3 2 1 17 5}

1.3 PKI PARTICIPANTS

The following are roles relevant to the administration and operation of the GPO-CA.

1.3.1 PKI Authorities

1.3.1.1 GPO PKI Policy Authority

The GPO PKI Policy Authority (PA) is a group of GPO personnel. The GPO-PKI-PA (or GPO-PA) is responsible for:

- The Government Printing Office Certification Authority (GPO-CA) Certificate Policy (CP)
- The GPO-CA Certification Practices Statement (CPS)
- Accepting applications from other PKI Domains desiring to interoperate with the GPO-CA
- Determining the mappings between certificates issued by applicant Entity CAs and the levels of assurance set forth in the GPO-CA-CP (which will include objective and subjective evaluation of the respective CP contents and any other facts deemed relevant by the GPO-PA)
- After a CA is authorized to interoperate with the GPO-CA, ensuring continued conformance of the Entity PKI Domain with applicable requirements is a condition for allowing continued interoperability with the GPO-CA

The GPO-PA will enter into an MOA with the applicant Entity setting forth the respective responsibilities and obligations of both parties, and the mappings between the certificate levels of assurance contained in this CP and those of the Entity CP. Thus, the term "MOA" as used in this CP shall always refer to the Memorandum of Agreement cited in this paragraph.

1.3.1.2 GPO Operational Authority

The GPO Operational Authority (OA) is the organization that operates the GPO-CA, including issuing GPO-CA certificates when directed by the GPO-PA, posting those certificates, Certificate Authority Revocation Lists (CARLs) and Certificate Revocation Lists (CRLs) into the GPO-CA repository, operating the OCSP system, and ensuring the continued availability of the repository to all users. The GPO-CA Operational Authority includes but is not limited to the following roles: Oversight Administrator, Officer, System Administrator, and Backup Operator, all described in later sections of this CP.

1.3.1.3 GPO Operational Authority Oversight Administrator

The OA Oversight Administrator (OAOA) is the individual within the GPO-OA who has principal responsibility for overseeing the proper operation of the GPO-CA including the GPO-CA repository, and who appoints individuals to the positions of GPO-CA Operational Authority (OA).

1.3.1.4 GPO Operational Authority Officers

These officers are the individuals within the GPO-OA, selected by the GPO-OAOA, who operate the GPO-CA and its repository including executing GPO-PA direction to issue CA certificates to CAs or taking other action to effect interoperability between the GPO-CA and Entity CAs.

1.3.1.5 Entity Certification Authority

An Entity wishing to interoperate with the GPO may apply for interoperation. Interoperation requires a mapping between the Entity CP and the GPO CP must be completed and an MOA must be in place. The Policy Mapping and MOA are put in place to ensure the level of security on the Entity CA is comparable to the GPO-CA and specify any additional requirements.

1.3.1.6 GPO Certification Authority

The GPO-CA is the entity operated by the GPO-OA that is authorized by the GPO-PA to create, sign, and issue public key certificates to Entity CAs. The GPO-CA is responsible for all aspects of the issuance and management of a certificate including:

- Control over the registration process
- The identification and authentication process
- The certificate manufacturing process
- Publication of certificates
- Revocation of certificates
- Re-key of GPO-CA signing material
- Ensuring that all aspects of the GPO-CA services, operations and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP

The Principal CA (PCA) is a CA within a PKI that has been designated to interoperate directly with Entity CAs, and which issues, either end-entity certificates, cross-certificates, or other means of interoperation. The PCA is the Root CA for the GPO PKI. Additionally, this CP may refer to CAs that are "subordinate" to the PCA. The GPO shall have at least one (1) Subordinate CA (SCA). The use of this term shall encompass any CA under the control of the PCA that has a certificate issued to it by the PCA or any CA subordinate to the PCA, whether or not a hierarchical or other PKI architecture is used.

1.3.1.7 GPO Registration Authority

The GPO Registration Authority (RA) is the entity that collects and verifies each End Entity's identity and information to be entered into his or her public key certificate. The GPO-RA performs its function in accordance with the GPO CPS approved by the GPO-PA. The requirements for GPO-RAs are set forth in the sections below.

1.3.1.8 GPO Naming Authority

The GPO Naming Authority is the entity that is responsible for managing the GPO name space.

1.3.2 Related Authorities

CAs operating under this CP will require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The GPO CPS shall identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.3.3 Trusted Agents

The trusted agent is a person who satisfies all the trustworthiness criteria of an RA and who performs identity proofing as a proxy for the RA. The trusted agent records information from and verifies biometrics (e.g., photographs, etc.) of credentials presented by applicants who cannot appear in person at an RA. The CPS will identify the parties that are authorized to provide such services and the mechanisms for determining their trustworthiness.

1.3.4 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the CP asserted in the certificate, and who does not issue certificates. Subscribers include all organizational personnel and, when determined by the GPO-PA, other individuals and possibly certain network or hardware devices such as firewalls and routers when needed for infrastructure protection. CAs are sometimes technically considered "subscribers" in a PKI. However, the term "Subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.5 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.6 Other Participants

The GPO-CA will require the participation of compliance auditors and assessors from time to time in accordance with this CP, and may involve participation from personnel in the information security community in accordance with this CP.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

Authorized applications are approved for the following security services provided by the GPO PKI:

- User Authentication
- Logical Access Control
- Secure Communication

- Digital Signature/Non-repudiation
- Card Authentication (card/token only; not presenter)

The GPO PA may identify additional authorized applications. This CP will be updated as new authorized applications are identified.

1.4.2 Prohibited Certificate Uses

Applications that attempt to use these certificates for services other than those identified are prohibited. Certificates that assert the id-fpki-common-cardAuth OID shall only be used to authenticate the hardware token containing the associated private key, and shall not be interpreted as authenticating the presenter of the token, or the holder of the token.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The GPO-PA is responsible for all aspects of this CP.

1.5.2 Contact Person

Questions regarding this CP shall be directed to the Chair of the GPO-PA, whose contact information and address can be found at the GPO PKI web site (http://www.gpo.gov/projects/pki.htm)., or to the designee of the Chair of the GPO-PA, the GPO Chief Information Security Officer, who can be reached by email at: pkisupport@gpo.gov.

1.5.3 Person Determining CPS Suitability for the Policy

The GPO-PA shall approve the GPO CPS. The GPO-PA is responsible for determining whether the GPO CPS conforms to the GPO CP, and in particular, properly adheres to any policy mappings approved by the GPO-PA between the GPO CP and an Entity CP.

1.5.4 CPS Approval Procedures

The GPO-PA shall approve the GPO CPS. The GPO-PA shall review the CPS at least once every year to determine if changes are required.

1.6 DEFINITIONS AND ACRONYMS

See sections 11 and 12 of this CP.

2. PUBLICATION OF CERTIFICATE INFORMATION

2.1 REPOSITORIES

The publication of data to the repositories will be appropriate to the certificate using community, and in accordance with the local security requirements. This includes information about certificate owners and organizations policies in addition to the directories containing the certificates and CRLs. Publication of certificates to the directories will constitute notification to all subscribers of the issuance of certificates. To facilitate the widest use of certificates, GPO may use an X.500 Directory System in addition to other repositories as deemed appropriate. The GPO CPS shall specify the location and contents of the repositories. The GPO-CA and its Operational Authority are responsible for the operation of all GPO-CA repositories.

2.2 PUBLICATION OF CERTIFICATE INFORMATION

2.2.1 Publication of Certificates and Certificate Status

The GPO-CA shall utilize a set of redundant directory systems and Online Certificate Status Protocol (OCSP) servers to achieve high availability and meet the availability requirements of the federal PKI Common Policy. This is achieved both by on-site redundant directory systems at the primary GPO-CA site, as well as backup directory systems, including an always online OCSP server, at the off-site backup location for the GPO-CA.

The GPO-CA shall ensure that certificates and CRLs are available for retrieval 24 hours per day, 7 days per week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually. This is achieved via the use of the redundant directory systems, and Change Control and other GPO-CA procedures.

2.2.2 Publication of CA Information

The GPO OA shall publish a copy of the GPO CP and the US Federal PKI Common Policy via the GPO PKI web site (http://www.gpo.gov/projects/pki.htm).

2.2.3 Interoperability

Certificates, CRL's and Certificate Status Servers of the GPO-SCA shall use standards based protocols, data structure, and directory schemas, to ensure that interoperability with the federal PKI infrastructure (the federal Common Policy and Federal Bridge CA) and relying parties is achieved.

2.3 TIME OR FREQUENCY OF PUBLICATION

This CP and any approved changes are published within 30 days of approval by the GPO PA.

Publication requirements for CRLs are described in sections 4.9.7 and 4.9.12 of this CP.

Certificates are published in the directory as soon as they are issued. CRLs and ARLs are published in the directory as soon as they are issued.

The automated replication mechanism used internal to the Directory is configured to replicate any changes to the onsite redundant directory systems as soon the changes occur. Replication to the off-site backup Directory system shall periodically not less than once per day.

2.4 ACCESS CONTROLS ON REPOSITORIES

The GPO-CA shall protect any repository information not intended for public dissemination or modification. Directory system access control mechanisms shall be used for this. Public keys and certificate status information in the GPO-CA repository shall be publicly available through the Internet.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

The GPO-CA asserting this CP (and when required the Entity CA) shall generate, sign and process certificates that contain an X.500 Distinguished Name (DN). Domain Component elements may be used in addition to the DN. Where DNs are required, subscribers shall have them assigned through their organizations, in accordance with a naming authority. If an X.500 Alternative Subject Name is used it must be marked non-critical. All CA and RA certificates shall have a non-null DN. The DN in all certificates shall accurately reflect organizational structure, and certificates for external agency DN's shall have the name of the agency involved in the DN.

3.1.2 Need for Names to be Meaningful

The identity certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way.

When DNs are used, it is preferable that the common name represents the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

The GPO-CA shall use DNs in certificates it issues. In the case where a root CA certifies a subordinate CA, the GPO-CA must impose restrictions on the name space authorized in the subordinate CA, which are at least as restrictive as its own name constraints.

Cross certificates issued by the GPO-CA at the Medium Assurance level shall have name constraints excluding the GPO name space (i.e. certificates issued by non-GPO CAs under the GPO name space are not trusted) specified by the GPO Naming Authority.

3.1.3 Anonymity or Pseudo-anonymity of Subscribers

The GPO-CA shall not issue anonymous certificates. The GPO-CA can issue pseudonymous certificates that identify subjects by their organizational role. The GPO-CA shall not issue any CA certificate that is anonymous or pseudonymous.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms shall be contained in the applicable certificate profile and are established by the GPO-PA.

3.1.5 Uniqueness of Names

Name uniqueness across the GPO-CA must be enforced. The GPO CAs and RAs shall enforce name uniqueness within the X.500 name space which they have been authorized. When other name forms are used, they too must be allocated such that name uniqueness across the GPO-CA is ensured.

The GPO shall document in its CPS:

- What name forms shall be used
- How the CAs and RAs will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys, then that party shall be required to prove possession of the private key that corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the GPO-CA. The GPO-CA or Entity CA shall then validate the signature using the party's public key. The GPO-PA may allow other mechanisms that are at least as secure as those cited here.

In the case where a key is generated directly on the party's token, or in a key generator that benignly transfers the key to the party's token, then the party is deemed to be in possession of the private key at the time of generation or transfer. If the party is not in possession of the token when the key is generated, then the token shall be delivered to the subject via an accountable method.

When keyed hardware tokens are delivered to certificate subjects, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subjects. The GPO must maintain a record of validation for receipt of the token by the

subject. When any mechanism that includes a shared secret is used, the mechanism shall ensure that the applicant and the GPO-CA are the only recipients of this shared secret.

3.2.2 Authentication of Organization Identity

Requests for GPO-CA certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization. The GPO-OA or GPO-RA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

3.2.3 Authentication of Individual Identity

Identity shall be authenticated, as described in the sub-sections below, depending on the type of Subscriber involved. There are different classifications of Subscribers and the initial registration process differs accordingly; however, all Subscribers are responsible for providing identity-proofing credentials as part of the initial registration process. A certificate shall be issued to a single end entity.

3.2.3.1 Authentication of Human Subscribers

For Subscribers, the Officer role (RAs and Security Officers) for the GPO-CA shall ensure that the applicant's identity information is verified and checked in accordance with the GPO CP and CPS. The GPO-RA shall ensure that the applicant's identity information and public key are properly bound. Additionally, the GPO-RA shall record the process that was followed for issuance of each certificate. The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identification
- A signed declaration by that person, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury), that he or she verified the identity of the Subscriber as required by the applicable certificate policy
- A unique identifying number from the ID of the verifier and, if in-person identity proofing is done, from the ID of the applicant
- The date and time of the verification
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

Identity for all human subscribers is established by in-person appearance before the Registration Authority,

Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D.

If an Applicant is unable to perform face-to-face registration alone (e.g., a network device), the applicant shall be represented by a human sponsor or trusted agent already issued a digital certificate by the GPO-CA. The human sponsor or trusted agent will present information

sufficient for registration of the certificate being requested, for both himself/herself and the applicant who the trusted person is representing.

3.2.3.1.1 Authentication for Role Based Certificates

There is a subset of human subscribers who may be issued role-based certificates. These certificates will identify a specific role on behalf of which the subscriber is authorized to act rather than the subscriber's name and are issued in the interest of supporting accepted GPO and external agency business practices. The role-based certificate can be used in situations where non-repudiation is desired. Normally, it will be issued in addition to an individual subscriber certificate. A specific role may be identified in certificates issued to multiple subscribers, however, the key pair will be unique to each individual role-based certificate. Roles for which role-based certificates may be issued are limited to those that uniquely identify a specific individual within an organization. Role-based certificates shall not be shared, but shall be issued to individual subscribers and protected in the same manner as individual certificates.

The GPO-CA shall record the information identified in Section 3.2.3.1 for a sponsor associated with the role before issuing a role-based certificate. The sponsor must hold an individual certificate in his/her own name issued by the GPO-CA at the same or higher assurance level as the role-based certificate.

The procedures for issuing role-based tokens must comply with all other stipulations of this GPO CP (e.g., key generation, private key protection, and Subscriber obligations).

For pseudonymous certificates that identify subjects by their organizational roles, the GPO-CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

3.2.3.2 Authentication of Devices

Some computing and communications components (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the component must have a human sponsor. The Sponsor is responsible for providing the following registration information:

- Equipment identification or service name
  - i) serial number (for devices)
  - ii) DNS and/or host name (for servers or components)
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)

- Contact information to enable the CA or RA to communicate with the sponsor when required

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the sponsor (using certificates of equivalent or greater assurance than that being requested).
- In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.1.

Identification and authentication of the human sponsor follows Section 3.2.3.1 as if the sponsor were applying for a certificate on their own behalf. In addition, the RA will verify the authority of the sponsor to receive certificates for that component (device) or server. The authority of the sponsor to receive device or server certificates is defined to be those personnel identified for this purpose in the agency's MOA with GPO, or by digitally signed message from those personnel in the MOA.

3.2.4 Non-Verified Subscriber Information

Only verified information (verified by the RA or CA personnel) shall be included in certificates.

3.2.5 Validation of Authority

Before issuing a certificate that asserts organizational identity, the GPO-CA shall validate that the subscriber (applicant) has the authority to act in the requested capacity. For pseudonymous certificates that identify subjects by their organizational role, the CA shall validate that the individual holds this role or has been delegated the authority to act or sign on behalf of that role.

3.2.6 Criteria for Interoperation

The GPO PA shall determine the interoperability criteria for CA's operating under this policy.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

The GPO-CA Trusted Role and Subscriber keys shall be automatically updated prior to expiration of the current key pairs. If more than nine (9) years have passed since the subscriber's identity was verified via in-person proofing (the procedures of section 3.1.9 above), then the certificate re-key shall require the same user identification proofing as certificate issuance.

The GPO-CA shall determine when certificate re-key operations will exceed the nine (9) year limitation and therefore prevent the automatic re-key and require the subscriber to present themselves in person for identity proofing per section 3.1.9 above. The CA performs a procedure described in detail in the CPS to accomplish this, which includes the following aspects.

a. A listing is created periodically that lists all Subscribers who will pass the 9 year mark within a certain lead time range.

b. All Subscribers on this list are sent an email informing them that they must present themselves for in-person identity proofing prior to the lead time expiring.

c. The listing also shows any Subscribers that are active that have passed the 9 year mark, and thus in theory could have an automatic re-key performed. These Subscribers have their certificate revoked by the RA, and an email is sent to the user informing them that their certificate has been revoked and they must present themselves for in-person identity proofing (per section 3.1.9 above) to obtain another certificate or to have key recovery performed.

3.3.2 Identification and Authentication for Re-key after Revocation

All GPO-CA Subscribers or human sponsors (in the case of device certificates) must repeat the initial certificate registration and request process, and the initial identify proofing process, in order to obtain a new certificate after a revocation.

3.4 Identification and Authentication for Revocation Request

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The following steps are required of a subscriber when applying for a GPO certificate:

- Establish need for certificate
- Establish identity of subscriber
- Obtain public and private key pairs for each certificate required
- Prove to the RA or CA that the Public key forms a functioning key pair with the private key that is held by the subscriber
- Provide a point of contact for verification of any roles or authorizations requested

CAs asserting to this CP shall certify Entity CAs (to include cross certification) only as authorized by the GPO-PA.

4.1.1 Who Can Submit a Certificate Application

4.1.1.1 CA Certificates

An application for a CA certificate shall be submitted by an authorized representative for the applicant CA.

4.1.1.2 User Certificates

An application for a user (subscriber) certificate shall be submitted by either the subcriber themselves, or by a trusted agent.

4.1.1.3 Device Certificates

An applicant for a device certificate shall be the human sponsor for the device.

4.1.2 Enrollment Process and Responsibilities

All communications between PKI authorities and other participants shall be protected from modification and authenticated; electronic communication of shared secrets shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms shall be used that are equivalent in strength to the public/private key pair involved. Out-of-band mechanisms shall protect the confidentiality and integrity of the information.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Delivery of Public Key for Certificate Issuance

Public keys must be delivered for certificate issuance in a way that binds the applicant verified identification to the public key. This binding may be accomplished using cryptography. If cryptography is used, it must be at least as strong as that employed in certificate issuance. Additionally this binding may also be accomplished using non-cryptographic physical and procedural mechanisms. These mechanisms may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request. The method used for public key delivery shall be defined in the GPO CPS.

In those cases where public/private key pairs are generated by the GPO-CA on behalf of the Subscriber, the GPO-CA shall implement secure mechanisms to ensure that the token on which the public/private key pair is held is securely sent to the proper Subscriber. The GPO-CA shall also implement procedures to ensure that the token is not activated by an unauthorized entity.

4.2.2 Approval or Rejection of Certificate Applications

Approval or rejection of certificate applications is at the discretion of the GPO PA or the PA's designee.

4.2.3 Time to Process Certificate Applications

Certificate applications must be processed and a certificate issued within 30 days of identity verification.

4.3 CERTIFICATE ISSUANCE

Upon receiving a request for a certificate, the GPO CA or RA shall respond in accordance with the requirements set forth in the GPO CP and CPS.

The certificate request may contain an already built ("to-be-signed") certificate. This certificate will not be signed until the process set forth in the GPO CP and CPS has been met.

While the Subscriber may do most of the data entry, it is still the responsibility of the RA to verify that the information is correct and accurate. This may be accomplished through a system approach linking trusted databases containing personnel information, or other equivalent authenticated mechanisms, or through personal contact with the Subscriber's sponsoring organization. If databases are used to confirm Subscriber information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought.

To the extent practical, certificates once created shall be checked to ensure that all fields and extensions are properly populated. This may be done through software that scans the fields and extensions looking for any evidence that a certificate was improperly manufactured.

The CA binds the identity information in the certificate application with the public keys during the certificate issuance process.

The Subscriber, shall use FIPS certified Commercial Off-the-Shelf (COTS) PKI software provided by the RA at Subscriber in person registration and identity proofing (see section 3.2.3.1 above), initiates a PKIX-CMP protocol session with the CA to start the certificate issuance process. The PKI COTS software PKIX-CMP protocol cryptographic parameters are used. SHA-256 is to be used with the COTS software PKIX-CMP protocol starting on January 1, 2008 and beyond. The PKIX-CMP protocol prevents interception of clear text data or substitution of data passed between the Subscriber's computer and the CA. The Reference Number and Authorization Code issued by the RA to the Subscriber during in-person identity proofing are entered by the Subscriber into the PKI COTS software at the Subscriber's PC, and this information uniquely identifies the Subscriber to the GPO-CA. The Subscriber's PKI COTS software cryptographic module (which meets FIPS 140 Security Level 1 requirements) generates the Subscriber's public/private verification key pair, and submits the public key to the CA for certification using PKIX-CMP protocol. Upon receipt of a valid certificate request from the Subscriber over the PKIX-CMP session, the GPO-CA automatically generates an encryption key pair and issues a signature verification public key certificate and an encryption public key certificate for that Subscriber, and this information is passed back to the Subscriber via the PKIX-CMP session.. The Subscriber certificates and the decryption private key, as well as the GPO-CA's verification certificate and the GPO PCA verification certificate, are provided to the Subscriber by the GPO-CA using the PKIX-CMP protocol to provide both integrity and privacy, which also includes a specific message via the user interface to the Subscriber indicating success or failure of certificate issuance.

For certificates issued to Subscribers on hardware tokens (smartcards, for example) for Medium-Hardware Assurance certificates, an authorized PKI RA shall issue the token to the subscriber.

The token shall be used along with the PKI COTS software, to interact with the CA using the PKIX-CMP protocol. The cryptographic parameters of the COTS software PKIX-CMP protocol are used. The token shall be created with the user present by the RA, then the user sets the password for the token, and the Subscriber then shall take possession of the token at the successful conclusion of the certificate registration and issuance process. The PKI COTS software, which interfaces to the smartcard via standard PCKS #11 interface and to the CA via the standard COTS PKIX-CMP protocol, shall be used by the RA in order to accomplish the key generation and certificate issuance process. The Subscriber's verification public/private key pair shall be generated by the smartcard and the public key shall be submitted to the CA, via the PKIX-CMP session between the COTS PKI software on the RA workstation. Upon receipt of a valid certificate request over the PKIX-CMP session, the GPO-CA shall automatically generate an encryption key pair and shall issue a signature verification public key certificate and an encryption public key certificate for that Subscriber, and this information shall be passed back to the token via the PKIX-CMP session. The 2 certificates shall then be loaded into the token, using the PKI COTS software, and the token is ultimately handed to the Subscriber by the RA at the successful conclusion of the certificate issuance and registration process. The OA staff, in the form of the RA, shall securely maintain the stock of hardware tokens prior to issuance. The token serial number of any token issued to a subscriber shall be recorded on the certificate registration paperwork. Tokens may be re-used for other subscribers once the key destruction process, using the vendor supplied initialization and key zeroization software, has been successfully implemented by an authorized RA . Tokens associated with a key compromise event shall not be re-used. The Certificate Revocation Request Form shall have a check box to indicate to the RA if the reason for Revocation is Key Compromise and also has the Serial Number of the token involved, if a token applies. In the event of key compromise, the token (smartcard) shall first be zeriozed using the vendor zeroization software utility, and then the RA shall physically destroy the smartcard by cutting it into at least 3 distinct pieces.

4.3.1 CA Actions During Certificate Issuance

Upon receiving a valid request, the CA/RA shall:

- Verify the identity of the requestor
- Verify the authority of the requestor and the integrity of the information in the certificate request
- Build and sign a certificate if all certificate requirements have been met
- Make the certificate available to the subscriber upon verifying that the subscriber has acknowledged their obligations

The GPO-CA does not sign the certificate until all identify verification and authentication procedures described in the GPO-CA CPS are completed. The responsibility for verifying prospective subscriber information shall be described in the GPO-CA CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The GPO-CA shall inform the Subscriber (or subject of the certificate) of the creation of the certificate and shall make the certificate available to the Subscriber. For device certificates, the human sponsor shall be informed by the GPO-CA.

4.4 CERTIFICATE ACCEPTANCE

A Subscriber shall be required to sign, using a handwritten signature, a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. The document shall contain the following requirements at a minimum:

- The Subscriber shall accurately represent themselves in all communications with the PKI authorities and other Subscribers.
- The Subscriber shall notify, in a timely manner, the CA that issued their certificates of suspicion that their private keys are compromised or lost, in the event that occurs.

4.4.1 Conduct Constituting Certificate Acceptance

No stipulation.

4.4.2 Publication of the Certificate by the CA

The GPO-CA shall publish Subscriber certificates into the GPO-CA Repository per section 2 of this CP, and also in accordance with section 9.4.3. The GPO-CA certificate shall be available in the GPO-CA Respository per section 2 of this CP.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The Federal PKI Policy Authority shall be notified by the GPO PA whenever a CA certificate is issued by the GPO-CA.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The intended scope of usage for the private key and associated certificate shall be specified through the use of certificate extension fields, including the key usage and extended key usage extension contained in issued certificates.

4.5.2 Relying Party Public Key and Certificate Usage

Certificates issued under this CP shall make use of certain critical extensions, including key usage and basic constraints, which relying parties are recommended to process and make use of in determining appropriate relying party use of GPO-CA issued certificates. In addition, the GPO-CA shall make available via the CRL and CSS service the status of certificates to relying parties, which relying parties are recommended to use in determining how to make use of any GPO-CA issued certificate.

4.6 CERTIFICATE RENEWAL

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but a new, extended validity period and a new serial number. Certificates may be renewed in order to reduce the size of CRLs. A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the renewed certificate must meet the requirements specified in Section 6.3.2. Certificates may also be renewed when a CA re-keys.

4.6.1 Circumstance for Certificate Renewal

Subscriber keys shall not be renewed except in situations of recovery from a CA key compromise. After certificate renewal, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.6.2 Who May Request Renewal

For all subordinate CA's and OCSP Responders operating under this policy, the GPO-CA Operating Authority may request renewal of the GPO CA or OCSP certificate. After certificate renewal, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.6.3 Processing Certificate Renewal Requests

No stipulation.

4.6.4 Notification of New Certificate Issuance to Subscriber

The CA shall notify the Subscriber of certificate renewal along with the content of the renewed certificate.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

All CA certificates shall be published in a GPO-CA repository as specified in section 2 above.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.

New certificates will need to be issued to Entity CAs by the GPO-CA when the GPO-CA re-keys. Upon re-key of this component, the GPO-CA shall identify and authenticate subscriber either by:

(a) Performing the initial registration identification process defined in Section 3.1, or

(b) If it has been less than three years since an Entity CA was identified as required in Section 3.1, using the currently valid certificate issued to the subscriber by the GPO-CA.

Subscribers of the GPO-CA shall identify themselves for the purpose of re-keying. The identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine (9) years from the time of initial registration.

After certificate rekey, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.7.1 Circumstance for Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains a new key. Examples of circumstances that require re-key include certificate expiration, compromise or loss, and issuance of a new hardware token.

4.7.2 Who May Request Certification of a New Public Key

Subscribers with a current, valid certificate may request re-key via a digitally signed message. CA's and RA's may request certification of a new public key on behalf of a subscriber. For device certificates, the human sponsor may request certification of a new public key for the device.

4.7.3 Processing Certificate Re-keying Requests

Digital signatures shall be validated on electronic re-key requests from subscribers. Alternatively, re-key requests may be validated using the procedures for subscriber identity and authentication for initial certificate issuance.

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6 Publication of the Re-keyed Certificate by the CA

CA certificates shall be published as required in section 2 of this CP. For subscriber certificates, there are no stipulations except for section 9.4.3 of this CP.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 CERTIFICATE MODIFICATION

Updating a certificate means creating a new certificate that has the same or a different key and a different serial number, and that it differs in one or more other fields, from the old certificate. For example, GPO-SCA may choose to update a certificate of a Subscriber whose characteristics have changed (e.g., name change due to marriage). The old certificate shall always be revoked, and therefore cannot be further re-keyed, renewed, or updated.

Further, if an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent in order for an updated certificate having the new name to be issued. The new certificate shall have a new public key for cases in which an individual's name changes.

4.8.1 Circumstance for Certificate Modification

The GPO-CA may modify a GPO CA or OCSP certificate whose characteristics have changed, for instance, to assert a new policy OID. The new certificate may contain the same public key or a new public key.

The GPO-CA may modify a subscriber's certificate due to a characteristic change of the subscriber (name change due to marriage, for example). The modified certificate shall contain a different public key.

4.8.2 Who May Request Certificate Modification

Subscribers with a current, valid certificate may request certificate modification via a digitally signed message. CA's and RA's may request certificate modification on behalf of a subscriber. For device certificates, the human sponsor may request certificate modification for the device.

4.8.3 Processing Certificate Modification Requests

If the subscriber's name has changed (for example, due to marriage), then the subscriber shall provide proof of the name change to the RA or trusted agent before the certificate modification is processed.

Proof of all subject information changes shall be provided to the RA or trusted agent before the modified certificate can be issued.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

CA certificates shall be published as required in section 2 of this CP. For subscriber certificates, there are no stipulations except for section 9.4.3 of this CP.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 CERTIFICATE SUSPENSION AND REVOCATION

4.9.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the subject and the subject's public key contained within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding include:

- Identifying information in the certificate has become invalid
- The Subscriber or CA can be shown to have violated, or is suspected of violating, the requirements of the GPO CP, or MOA
- The private key has been or is suspected of having been compromised, or has been lost, stolen, or destroyed in a fashion where there is potential for compromise or loss of control over the use of the private key

Additionally, a Subscriber may always request the revocation of his or her certificate directly. Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information at least until the certificates expire.

4.9.2 Who Can Request Revocation

A GPO-CA issued certificate may be revoked at the direction of the GPO-PA, or an authenticated request by the RA, subscriber, or a designated official. (the designated official shall be identified and authorized in the GPO CP, CPS, or MOA to make such a request).

The process for requesting revocation of a Subscriber certificate issued by the GPO-CA shall be set forth in detail in the GPO CPS. Revocation normally will proceed once:

- The GPO-CA receives sufficient evidence of compromise or loss of the subscriber's corresponding private key

- An authenticated request is made to the GPO-CA by the holder of the private key
- Someone in his or her supervisory chain, or an officially designated administrative or information security officer, makes an authenticated request for revocation

4.9.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). Only the GPO-PA may direct the GPO-OA to revoke certificates issued by the GPO-CA.

Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties. In particular, if the revocation is being requested for reason of key compromise or suspected fraudulent use, then the Subscriber's or the RA's revocation request must so indicate. If a RA performs this on behalf of a Subscriber, a formal, signed message format known to the CA shall be employed. All requests shall be authenticated; for signed requests from the certificate subject, or from an RA, verification of the signature is sufficient.

Upon receipt of a revocation request involving a GPO-CA issued certificate, the GPO-OA shall authenticate the request and apprise the GPO-PA. The GPO-PA may, at its discretion, take whatever measures it deems appropriate to verify the need for revocation. If the revocation request appears to be valid, the GPO-PA shall direct the GPO-CA to revoke the certificate by placing its serial number and other identifying information on a CARL/CRL and then post the CARL/CRL in the GPO-CA repository, in addition to any other revocation mechanisms used. The GPO-PA at its discretion may set forth emergency procedures for the GPO-CA to use to effect immediate revocation of a certificate issued by the GPO-CA when appropriate.

For PKI implementations using hardware tokens, a Subscriber ceasing its relationship with an organization that sponsored the certificate shall, prior to departure, surrender to the organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. If a Subscriber leaves an organization all the Subscriber's certificates shall be immediately revoked. The token shall be zeroized or destroyed upon, surrender and shall be protected from malicious use between surrender and zeroization or destruction.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation requests. The GPO-CA shall revoke certificates upon request as quickly as is practical. Revocation requests shall be processed and the CRL updated prior to the next CRL issuance, unless the revocation request is received within 2 hours of the next regularly scheduled CRL issuance. In that event (that the revocation request is received within 2 hours of the next regularly scheduled CRL issuance), the revocation shall be processed by the following CRL issuance.

4.9.5 Time within which CA must Process the Revocation Request

The GPO-CA shall revoke certificates as quickly as practical after a valid revocation request is received. Revocation requests shall be processed before the next CRL is published, excepting those requests which are received within two (2) hours of CRL publication. Revocation requests received within two (2) hours of CRL issuance shall be processed before the following CRL is published.

4.9.6 Revocation Checking Requirements for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL Issuance Frequency

CRLs shall be issued in accordance with the following frequency requirements:

- CAs that only issue certificates to CAs and that operate offline must issue CRLs at least once every 24 hours, and the *nextUpdate* time in the CRL may be no later than 24 hours after issuance time.
- CAs that issue certificates to subscribers or operate online must issue CRLs at least once every 18 hours, and the *nextUpdate* time in the CRL may be no later than 18 hours after issuance time.

Certificate status information may be issued more frequently than the issuance frequency described above. CRLs shall be issued within 18 hours of notification of loss or compromise of private key. The GPO-CA shall ensure that superseded certificate status information is removed from the repository upon posting of the latest certificate status information.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation. The GPO shall coordinate with the repositories to which they post certificate status information to reduce latency between creation and availability. Superseded certificate status information shall be removed from the repository system upon posting of the latest certificate status information.

4.9.8 Maximum Latency for CRLs

CRL's shall be published within four (4) hours of generation. Each CRL is published with the *nextUpdate* time specified in the previous CRL for the same scope.

4.9.9 On-line Revocation/Status Checking Availability

The GPO-CA shall support, in addition to CARL/CRLs, on-line status checking via the On-line Certificate Status Protocol (OCSP). Client software using on-line status checking need not obtain or process CARL/CRLs.

4.9.10 On-line Revocation Checking Requirements

The GPO-SCA does support on-line revocation/status checking using the OCSP protocol. Certificate status checking via the OCSP protocol can be performed for all OID types that are supported by the GPO-SCA..

OCSP data is updated every 30 minutes by the CA. The OCSP data available to relying parties is synchronized with the CA CRL every 30 minutes. Therefore, any certificate revocation is available to relying parties within 30 minutes of placement on the CRL.

A verification (signing) key issued by the GPO-SCA is used for the purpose of signing OCSP response messages.

Error messages in response to certificate status requests are not signed, as provided for in the IETF OCSP standard, RFC 2560.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related To Key Compromise

In the event of a GPO-CA private key compromise (confirmed or suspected) or loss, or Subscriber certificate is revoked because of compromise or suspected compromise, the GPO-CA shall publish a CARL and CRL within 18 hours of notification to the GPO-CA.

4.9.13 Circumstances for Suspension

Suspension shall not be used by the GPO-CA.

4.9.14 Who Can Request Suspension

Suspension is not permitted by the GPO-CA, therefore there is no stipulation.

4.9.15 Procedure for Suspension Request

Suspension is not permitted by the GPO-CA, therefore there is no procedure for suspension request.

4.9.16 Limits on Suspension Period

Suspension is not permitted by the GPO-CA, therefore there is no stipulation.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

The GPO-CA shall provide CSS service via an online OCSP Responder in accordance with federal PKI Common Policy requirements and standard protocols.

4.10.2 Service Availability

The CSS for the GPO-CA shall be available online and shall have an off-site backup system that is also online to provide operational resiliency and high availability to meet all federal PKI requirements.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

CA keys are never escrowed.

Signature keys, including any Subcriber private dual use keys, are never escrowed.

Subscriber dual use keys shall never be escrowed.

Subscriber key management keys are available for key recovery using the practices of the GPO-CA CPS.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The GPO-CA does not offer or perform this service/function and there are no stipulations.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

The GPO-CA shall impose physical security requirements that provide similar levels of protection as those specified below. All the physical control requirements apply equally to the GPO-CA.

GPO-RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the GPO-RA equipment environment.

The GPO-CA equipment shall be in a controlled facility that is monitored 24 hours per day, 7 days per week, 52 weeks per year. The GPO-CA cryptographic modules, both those active and operational, and those stored in security containers for on-site and off-site backup, shall be protected against theft, loss, and unauthorized use by the controls specified in section 5.1.2 below.

5.1.1 Site Location and Construction

The location and construction of the facility housing the GPO-CA equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the GPO-CA equipment and records.

5.1.2 Physical Access

The GPO-CA equipment shall always be protected from unauthorized access, and especially while the cryptographic module is installed and activated. Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.

5.1.2.1 Physical Access for CA Equipment

The CA equipment is located in a secure PKI facility (at both the primary site and off-site backup location) which provides extensive controls over physical access.

Physical access controls and procedures shall be implemented to:

- Ensure no unauthorized access to the CA hardware is permitted
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers so as to ensure all GPO-CA media is protected from unauthorized physical access
- electronically monitor for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require via technical enforcement two-person physical access control to both the cryptographic module and computer system

An integrated physical access control and intrusion detection system shall be operational to restrict access to authorized personnel, to detect unauthorized access, and to provide for the audit of all entries to and exits from the controlled areas. Sensors shall be operational to monitor exit and entrance doors.

Removable cryptographic modules shall be inactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules and GPO-CA equipment shall be placed in secure containers. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

A security check of the facility housing the GPO-CA equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation
- Any security containers are properly secured
- Physical security systems (e.g., door locks, vent covers) are functioning properly
- The area is secured against unauthorized access

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, both of the last two authorized personnel, to depart, will perform the check together, and both shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 Physical Access for RA Equipment

Registration Authority equipment shall be protected from unauthorized access while the cryptographic module is installed via the password required for all RA tokens, which are required to be FIPS 140 Level 2 compliant hardware tokens. Only the authorized user can access

the cryptographic module for RA operations, and the RA shall ensure that no other party uses the RA equipment while the RA is logged in. The RA user shall ensure that the Level 2 hardware token is controlled at all times, by having the token in the RA's possession or in a locked cabinet/desk .

5.1.2.3 Physical Access for CSS Equipment

The CSS equipment shall be located in the same secure PKI facility as the CA equipment (at both the primary and off-site backup location), which shall provide the same controls as to the CA equipment.

5.1.3 Power and Air Conditioning

The GPO-CA shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. The directories (containing CA issued certificates and CARLs) shall be provided with uninterrupted power sufficient for a minimum of six (6) hours of operation in the absence of commercial power.

5.1.4 Water Exposures

The GPO-CA and CSS equipment shall be installed such that it is not in danger of exposure to water.

5.1.5 Fire Prevention and Protection

The GPO-CA secure facility is fully wired for fire detection, alarm and suppression. Routine, frequent inspections of all systems shall be made to assure adequate operation.

5.1.6 Media Storage

GPO-CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the GPO-CA.

5.1.7 Waste Disposal

Paper documents shall be shredded using a cross-cut shredder that complies with NSA/CSS 02-01. Digital information on digital media that is to be disposed of is first sanitized using COTS software, which shall comply with DoD and FIPS standards for information clearing/sanitization. Digital media that is to be destroyed shall be destroyed in accordance with DoD Standard 5220.22- M. Hard disks shall be mechanically destroyed after all information is sanitized.

Magnetic tape shall be destroyed by first cutting the tape into at least 4 pieces and then running at least 2 of the pieces through a cross-cut shredder.

5.1.8 Off-Site Backup

The GPO-CA requires, full system backups, sufficient to recover from system failure, shall be made on a periodic schedule. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an offsite location (separate from the GPO-CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational GPO-CA.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the GPO-CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

At a minimum the following roles will be used:

1. *GPO-OA System Administrator (GPO-OASA)* – authorized to install, configure, and maintain the CA; establish and maintain user accounts; and configure audit parameters

2. *GPO-OA Officer – Master Users* – authorized to configure certificate profiles; and generate component keys

3. *GPO-OA Officer – Security Officers* – authorized to manage (including issuance and revocation) Cross certificates, CA certificate and Trusted Role Subscriber certificates

4. *GPO-OA Officer– Registration Authority* – authorized to request or approve subscriber certificates or subscriber certificate revocations

5. *GPO-OA Officer – Directory Administrators* – maintaining the PKI entries in the certificate repository

6. *GPO Security Compliance Auditor* – authorized to view and maintain audit logs

7. *GPO-OA Backup Operator (GPO-OABUO)* – authorized to perform system backup and recovery

5.2.1.1 GPO-OA System Administrator

The administrator role is responsible for:

- installation, configuration, and maintenance of the CA
- establishing and maintaining CA system accounts
- configuring audit parameters

GPO-OASAs do not issue certificates to subscribers.

5.2.1.2 GPO OA Officer – Master Users

The OA Officer - Master Users are responsible for:

- configuring certificate profiles or templates
- generating and backing up CA keys

5.2.1.2.1 GPO OA Officer – Security Officers

The OA Officer - Security Officers are responsible for:

- registering new Trusted Role Subscribers and requesting the issuance of certificates
- verifying the identity of Trusted Role Subscribers and accuracy of information included in certificates
- approving and executing the issuance of Cross certificates, CA certificates and Trusted Role Subscriber certificates
- requesting, approving and executing the revocation of Cross certificates, CA certificates and Trusted Role Subscriber certificates

5.2.1.2.2 GPO OA Officer – Registration Authorities (RAs)

The OA Officer – Registration Authority (RAs) Administrators are responsible for:

- registering new subscribers and requesting the issuance of certificates
- verifying the identity of subscribers and accuracy of information included in certificates
- approving and executing the issuance of subscriber certificates
- requesting, approving and executing the revocation of subscriber certificates

5.2.1.2.3 GPO OA Officer – Directory Administrators

The OA Officer - Directory Administrators are responsible for maintaining the PKI entries in the certificate repository. The Directory Administrator can be an OA Officer – Security Officer or OA Officer – Administrator, but may **not** be an OA Officer – Master User or a Security Compliance Auditor.

5.2.1.3 GPO Security Compliance Auditor

The auditor role is responsible for:

- reviewing, maintaining, and archiving audit logs
- performing or overseeing internal compliance audits to ensure that the GPO-CA is operating in accordance with this CP and the CPS

This role can have no other trusted role in the GPO PKI.

5.2.1.4 GPO Backup Operator

The operator role is responsible for the CA equipment system backups and recovery or changing recording media. This role can be performed by the OA Officer-Administrator.

5.2.2 Number of Persons Required Per Task

Multi person control is implemented to prevent accidental or malicious actions involving the GPO-CA. At a minimum the following actions require 2 or more individuals holding Trusted Roles (multi-party control for logical access operations cannot include the Auditor Trusted Role and in addition, where multi-party control for logical access is required, at least one of the parties shall be an Administrator.):

- Generation of GPO-CA Signing Keys
- Activating GPO-CA Signing Keys
- Using GPO-CA Signing Keys
- Deactivating GPO-CA Signing Keys
- Backing up or Duplicating GPO-CA Private Signing Keys
- Physical Control of Backups of GPO-CA Signing Keys
- Physical Access or Control of the Cryptographic Module
- Physical Access or Control of the GPO-CA
- Physical Access or Control of the Safes and/or Secure Containers
- Physical Access to the GPO-CA
- Audit Log Review and Oversight
- Recovery of a subscribers encryption private key for a third party as directed by the GPO-CA Policy Authority or legal judgment

5.2.3 Identification and Authentication for Each Role

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4 Roles Requiring Separation of Duties

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means. The separation provides a set of checks and balances over the GPO-CA operation.

CA personnel shall be specifically designated to the roles defined in Section 5.2.1 above. Individuals may assume more than one role, however, individuals who assume a Security Compliance Auditor role may not hold any other trusted role, individuals who assume an Officer role may not assume a System Administrator role (i.e. an Officer may also be a Backup Operator, a System Administrator may also be a Backup Operator). Individuals may not assume more than one of the following roles: OA Officer – Master User, OA Officer – Security Officer, or OA Officer – Administrator. The OA Officer – Directory Administrator may be an OA Officer – Security Officer or OA Officer – Registration Authority but may not be an OA Officer – Master User. The CA system shall identify and authenticate its users and shall ensure that no user identity can assume a Security Compliance Auditor role and any other role, or both a System Administrator and an Officer role. No individual shall be assigned more than one identity.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens. The detail requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA shall be set forth in the GPO CPS.

There are no security clearance requirements in this CP. The GPO CPS will specify GPO-CA personnel security clearances stipulations that may exceed these requirements.

5.3.2 Background Check Procedures

The GPO-CA shall conduct background checks on personnel that hold Trusted Roles that includes checks for the following:

- Employment
- education
- references
- place of residence
- credit checks
- criminal record checks (law enforcement)

All personnel that fill a GPO-CA Trusted Role shall have a NAC-I background check conducted that is suitably adjudicated in accordance with federal law. The NAC-I check shall go back at least five (5) years. The highest level educational degree obtained shall be verified. Place of

residence checks shall go back at least three (3) years. The GPO Personnel Security Office shall conduct all background and NAC-I checks in accordance with federal law.

An active, current GPO security clearance (Secret, or Top Secret or above) may be used in lieu of the personnel screening identified above to establish that a NAC-I background check is conducted that is suitably adjudicated in accordance with federal law, since a GPO security clearance at the Secret, Top Secret or above level requires a full scope SSBI background investigation that meets and exceeds the NAC-I requirements, and to keep a GPO security clearance active requires that it be renewed (and another background check conducted) at least every five (5) years. Thus, an active GPO security clearance at the Secret, Top Secret or above level meets or exceeds the NAC-I background check requirements.

.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the GPO-CA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA/RA security principles and mechanisms
- All PKI software versions in use on the GPO-CA system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures
- Physical Security Procedures

5.3.4 Retraining Frequency and Requirements

Individuals responsible for GPO-CA roles shall be aware of changes in the GPO-CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are GPO-CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Any person that operates in violation of this CP or the CPS or the practices and procedures stated herein, whether through negligence or with malicious intent, shall have privileges revoked and may be subject to administrative and disciplinary action. Violations of this CP or the CPS that are determined by the GPO Operational Authority based on a fact based investigation to be due to malicious intent, shall subject to some form of administrative or disciplinary action, which shall be documented in writing by the GPO OA. Repeated or significant violation of the CP or CPS requirements shall result in privilege revocation and disciplinary action, which shall be documented in writing by the GPO OA. The range of disciplinary actions available shall include termination.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the GPO-CA shall meet applicable requirements set forth in section 5.3.1 above. Vendors who provide services to the GPO PKI shall establish procedures to ensure that any subcontractors who directly provide services to the GPO PKI perform in accordance with the requirements of section 5.3.1 above.

5.3.8 Documentation Supplied to Personnel

The GPO-CA shall make available to its CA and RA personnel the certificate policies it supports, relevant parts of the GPO CPS, and any relevant statutes, policies or contracts. Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.4 AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to the security of the GPO-CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Sections 5.4.3 and 5.5.2 of this CP below.

5.4.1 Types of Events Recorded

All security auditing capabilities of the GPO-CA operating system and PKI CA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. (Note: the table below may be replaced in future releases of this CP with a reference to the Certificate Issuing and Management Components Protection Profile being developed by NIST.) At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- Type of event
- Date and time the event occurred
- Success or failure indicator when executing the GPO-CA signing process
- Success or failure indicator when performing certificate revocation
- Identity of the entity and/or operator (of the GPO-CA) that caused the event
- Message from any source requesting an action by the GPO-CA is an auditable event (message must include message date and time, source, destination and contents)

Auditable Event
SECURITY AUDIT
Any changes to the Audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the Audit logs
IDENTIFICATION AND AUTHENTICATION
Successful and unsuccessful attempts to assume a role
Change in the value of maximum authentication attempts
Maximum number of unsuccessful authentication attempts during user login
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
An Administrator changes the type of authenticator, e.g., from password to biometrics
KEY GENERATION
Whenever the GPO-CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
PRIVATE KEY LOAD AND STORAGE
The loading of Component private keys
All access to certificate subject private keys retained within the GPO-CA for key recovery purposes
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE
All changes to the trusted public keys, including additions and deletions
PRIVATE KEY EXPORT
The export of private keys (keys used for a single session or message are excluded)
CERTIFICATE REGISTRATION
All certificate requests
CERTIFICATE REVOCATION
All certificate revocation requests
CERTIFICATE STATUS CHANGE APPROVAL
The approval or rejection of a certificate status change request
GPO-CA CONFIGURATION

Auditable Event
Any security-relevant changes to the configuration of the GPO-CA
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified
CERTIFICATE PROFILE MANAGEMENT
All changes to the certificate profile
REVOCATION PROFILE MANAGEMENT
All changes to the revocation profile
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT
All changes to the certificate revocation list profile
LOCAL DATA ENTRY
All security-relevant data that is entered in the system
REMOTE DATA ENTRY
All security-relevant messages that are received by the system
DATA EXPORT AND OUTPUT
All successful and unsuccessful requests for confidential and security-relevant information
MISCELLANEOUS
Installation of the Operating System
Installation of the GPO-CA
Installing hardware cryptographic modules
Removing hardware cryptographic modules
Destruction of cryptographic modules
System Startup
Logon Attempts to GPO-CA Apps
Receipt of Hardware / Software
Attempts to set passwords

Auditable Event
Attempts to modify passwords
Backing up GPO-CA internal database
Restoring GPO-CA internal database
File manipulation (e.g., creation, renaming, moving)
Posting of any material to a repository
Access to GPO-CA internal database
All certificate compromise notification requests
Loading tokens with certificates
Shipment of Tokens
Zeroizing tokens
Rekey of the GPO-CA
Configuration changes to the CA server involving:
Hardware
Software
Operating System
Patches
Security Profiles
Appointment of an individual to a trusted role
Designation of personnel for multi-party control
PHYSICAL ACCESS / SITE SECURITY
Personnel Access to room housing GPO-CA
Access to the GPO-CA server
Known or suspected violations of physical security
ANOMALIES
Software Error conditions
Software check integrity failures
Receipt of improper messages
Misrouted messages
Network attacks (suspected or confirmed)

Auditable Event
Equipment failure
Electrical power outages
Uninterruptible Power Supply (UPS) failure
Obvious and significant network service or access failures
Violations of Certificate Policy
Violations of Certification Practice Statement
Resetting Operating System clock

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed at least once every week. All significant events shall be explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

A statistically significant set of security audit data generated by the GPO-CA, since the last review, shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. For the GPO-CA, at least 70% of security audit data generated by the GPO-CA since the last review shall be examined.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least two months as well as being retained in the manner described below. The individual who removes audit logs from the GPO-CA system shall be an official different from the individuals who, in combination, command the GPO-CA signature key.

The audit log data is kept live on the CA or RA hardware and archived as specified below.

5.4.4 Protection of Audit Log

The audit process shall not be done by or under the control of the GPO-OA. GPO-CA system configuration and procedures must be implemented together to ensure that:

- only authorized people have read access to the logs
- only authorized people may archive audit logs
- audit logs are not modified

The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (If a system over-writes audit logs after a given time, the audit log is not considered deleted or destroyed if the audit log has been backed up and archived). Audit logs shall be moved to a safe, secure storage location separate from the GPO-CA equipment.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least weekly. A copy of the audit log shall be sent off-site in accordance with the GPO CPS on a weekly basis.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the GPO-CA. Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the GPO-OA shall determine whether to suspend GPO-CA operation until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

The Operational Authority will perform routine self assessments of security controls.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Events Archived

GPO-CA archive records shall be sufficiently detailed to establish the proper operation of the GPO-CA, or the validity of any certificate (including those revoked or expired) issued by the GPO-CA.

At a minimum, the following data shall be recorded for archive:

Data To Be Archived
CA accreditation (if applicable)
Certificate Policy
Certification Practice Statement

Data To Be Archived
Contractual obligations
Other agreements concerning operations of the CA
System and equipment configuration
Modifications and updates to system or configuration
Certificate requests
Revocation requests
Subscriber identity Authentication data as per Section 3.2.3
Documentation of receipt and acceptance of certificates
Subscriber Agreements
Documentation of receipt of tokens
All certificates issued or published
Record of CA Re-key
All CRLs issued and/or published
Other data or applications to verify archive contents
Compliance Auditor reports
Any changes to the Audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the Audit logs
Whenever the CA generates a key (Not mandatory for single session or one-time use symmetric keys)
All access to certificate subject private keys retained within the CA for key recovery purposes

5.5.2 Retention Period for Archive

Archive data must be retained for a minimum of 10 years and 6 months. Executive branch agencies must follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.

This minimum retention period for these records is intended only to facilitate the operation of the GPO-CA.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Alternatively, an Entity may retain data using whatever procedures have been approved by NARA for that category of documents. Applications that are required to process the archive data shall also be maintained for a period determined by the GPO-PA for the GPO-CA.

Prior to the end of the archive retention period, the GPO-CA shall provide archived data and the applications necessary to read the archives to a GPO-PA approved archival facility, which shall retain the applications necessary to read this archived data.

5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the GPO-CA, archived records may be moved to another medium when authorized by the GPO-OA. The contents of the archive shall not be released except as determined by the GPO-PA for the GPO-CA or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the GPO-CA.

5.5.4 Archive Backup Procedures

Archive files shall be backed up along with the security audit logs.

Paper archives shall be backed up to microfiche, or scanned digitally to digital media, or other long-term storage solution. The GPO-CA CPS shall specify the details of which media type is used, the frequency and other procedural details. The CPS shall also specify how archive backup files are managed.

5.5.5 Requirements for Time-Stamping of Records

CA records shall be time stamped as they are created. Time-stamping of records is accomplished via the GPO-CA system, using the GPO-CA system clock. The GPO-CA system clock is synchronized on a periodic basis with the NIST official time source, using the IETF standard Network Time Protocol (NTP), or equivalent process/time source, to ensure that the CA system clock is accurate. The NTP service is set for automatic service startup on the CA system to ensure that the NTP service is always started whenever the CA sysem must be started.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store the GPO-CA archive information shall be published in the GPO CPS.

5.6 KEY CHANGEOVER

To minimize risk from compromise of a GPO-CA's private signing key, that key may be changed ; from that time on, only the new key will be used for certificate signing purposes. The older, but still valid, GPO-CA certificate will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. Following GPO-CA key changeover, only the new GPO-CA key will be used to sign CRLs and certificates going forward. The new CA key shall comply with the validity period requirements in section 6.3.2 of this CP. The GPO-CA uses key rollover certificates using the facilities of the Entrust COTS PKI software (which is FIPS certified) and the Safenet HSM (also FIPS certified) to accomplish CA key changeover. The old CA key is held and protected using the same mechanisms as the new CA key, which shall utilize the Safenet LunaSA HSM (which shall be FIPS certified to Level 3) and the Entrust COTS PKI software.

The Subscriber certificates issued by the GPO-CA shall be capable of automatic key roll-over. As such, the encryption and digital signature key pairs of the Subscriber shall be automatically updated prior to expiry.

5.7 COMPROMISE AND DISASTER RECOVERY

In any key compromise situation, a report will be filed with the GPO PA indicating the circumstances under which the compromise occurred. The Federal PKIPA shall be notified by GPO PA in every confirmed instance of a key compromise.

5.7.1 Incident and Compromise Handling Procedures

The GPO Computer Security Incident Response Team (CSIRT) Procedures shall be used by the GPO PA and GPO OA when handling incidents or compromise events. These procedures are included in the GPO PCA and SCA CPS by reference.

These procedures include the following steps:

- Report and document the incident (by using the GPO IT Help Desk ticketing system) (All steps for responding to the incident in the following steps will be documented also)
- Identify the nature and scope of the incident
- Notification of the incident and its associated potential impacts and affects to stakeholders (Federal PKIPA, Subscribers, PA, OA, and Relying Parties)
- Protecting Evidence and Logs

- Containment of the results and affects of the incident to reduce adverse impacts
- Eradication of the causes and sources of the incident and any adverse results
- Recovery to restore the GPO-SCA to effective and efficient operations
- Follow-up to notify stakeholders (Federal PKIPA, Subscribers, GPO PA, GPO OA and Relying parties) of the results of the recovery from the incident and GPO-SCA operational status
- Post-incident review to ensure lessons learned are incorporated into future operations and practices

5.7.2 Computing Resources, Software, and/or Data are Corrupted

If GPO-CA equipment is damaged or rendered inoperative, but the GPO-CA signature keys are not destroyed, GPO-CA operation shall be reestablished as quickly as possible, giving priority to the ability to generate certificate status information. The integrity of the system shall be ensured at all times as GPO-CA equipment/systems are restored to operation.

5.7.3 GPO-CA Private Key Compromise Procedures

If the GPO-CA signature keys are compromised or lost (such that compromise is possible even though not certain):

- The GPO-PA and all of its member organizations shall be securely notified as soon as practical (so that Entities may issue CARLs revoking any cross-certificates issued to the GPO-CA)
- A new GPO-CA key pair shall be generated securely by the GPO-CA in accordance with the requirements of this CP and the procedures set forth in the GPO-CA CPS
- New GPO-CA certificates shall be issued in accordance with the requirements of this CP (including section 6.1.4 for any self-signed CA certificates) and as specified in the GPO-CA CPS.

The GPO-CA Operational Authority (OA) shall also investigate and report to the GPO-PA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

In the event of the compromise of the GPO-CA private key, the federal PKI PA will be informed via secure communication from the OA. The CA installation shall be reestablished in accordance with any instructions and direction from the GPO OA and the GPO PKI Policy Authority. In general, the OA shall revoke the certificates for the GPO-CA, install a new GPO-CA, generate a new GPO-CA certificate, and publish the new GPO-CA certificate to the directory. The OA shall review all MOA's that exist and make determination of any other CA's that may cross-certified, and then notify each and every one of any CA's that are cross-certified.

The OA shall notify the Subscribers of the GPO-CA of the key compromise via a secure communication. The Subscriber certificates shall be renewed automatically by the GPO-CA under the new CA key pair, using the capabilities of the CA software. The fingerprint of the new

GPO-CA key pair shall be placed onto the GPO PKI web site (http://www.gpo.gov/projects/pki.htm) and all Subscribers instructed by email from the GPO PKI service that this fingerprint can be validated as a backup method to ensure that the proper new CA key is installed.

5.7.3.1 GPO-CA Signature Keys are Revoked

If the GPO-CA cannot issue a CARL/CRL prior to the time specified in the next update field of its currently valid CARL/CRL, then the GPO-PA and all of its members shall be securely notified as soon as practical. The GPO-CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the GPO CPS. The GPO-CA shall, as soon as practical, securely advise the GPO-PA and all of its member organizations in the event of a disaster where the GPO-CA installation is physically damaged and all copies of the GPO-CA signature keys are destroyed.

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby the GPO-CA installation is physically damaged and all copies of the GPO-CA signature key are destroyed as a result, the GPO-PA and all of its member agencies shall be securely notified as soon as practical, and the GPO-PA shall take whatever action it deems appropriate. Relying Parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of GPO-CA operation with new certificates.

5.8 CA OR RA TERMINATION

In the event of termination of the GPO-CA operation, certificates signed by the GPO-CA shall be revoked and the GPO-PA shall advise agencies that have entered into MOAs with the GPO-PA, prior to termination, that GPO-CA plans to terminate operation so they may revoke certificates they have issued to the GPO-CA. All affiliated entities (agencies) shall be be notified by the GPO-PA prior to termination of the GPO-CA. Prior to GPO-CA termination, the GPO-CA shall provide archived data to a GPO-PA approved archival facility.

In the event that the GPO-CA terminates operation, the GPO-CA shall ensure that any certificates issued to the GPO-CA have been revoked.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 GPO-PKI and GPO-CA Key Pair Generation

Cryptographic keying material for certificates issued by the GPO-CA shall be generated in FIPS 140 validated cryptographic modules. For the GPO-CA, the modules shall meet or exceed Security Level 3.

The GPO-CA and Entity CAs must document their key generation procedure in their CPSs, and generate auditable evidence that the documented procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. The process shall be validated by an independent third party.

6.1.1.2 Subscriber Key Pair Generation

For subscribers, software or hardware shall be used to generate pseudo-random numbers, key pairs and symmetric keys. Any pseudo-random numbers used for key generation material shall be generated by a FIPS approved method.

6.1.1.3 CSS Key Pair Generation

The CSS shall generate its key pair in a FIPS 140 compliant module that is certified to Level 2 or above.

6.1.2 Private Key Delivery to the Subscriber

The GPO-CA generates its own key pair and therefore does not need private key delivery. Private decryption keys shall be delivered by the GPO-CA using the security protection provided by PKIX-CMP protocol in the COTS PKI software, and shall use cryptographic algorithms in the PKIX-CMP that are as strong or stronger than the 2048 bit RSA public/private key pairs. The GPO Operational Authority shall use the COTS software capabilities for PKIX-CMP, or equivalent, which shall provide strong encryption algorithms and key sizes that are as strong or stronger than the 2048 bit RSA public/private key pairs used by the GPO-CA, to protect these RSA private decryption keys.

For Subscribers that will have Medium-Hardware Assurance certificates, the private decryption keys shall be stored in a hardware module that meets FIPS 140-2 Level 2 requirements.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys shall be delivered to the certificate issuer electronically in a certificate request in accordance with PKIX-CMP protocol. The COTS PKI software shall be used by the GPO-CA for its Subscribers to provide appropriate encryption and integrity cryptographic mechanisms in compliance with the PKIX-CMP protocol, which are cryptographically as strong or stronger than the 2048 bit RSA public keys that are requested for certification. All GPO-CA Subscribers are required to use the PKI COTS software.

For Subscrsibers that will have Medium-Hardware Assurance certificates, the public key delivery process shall use a hardware module that meets FIPS 140-2 Level 2 requirements.

6.1.4 GPO-CA Public Key Delivery to Relying Parties

The GPO-CA shall post the certificates it issues in the GPO-CA repository. For Entity CAs to issue cross-certificates to the GPO-CA, the GPO-CA shall transport its public key to the Entity CA in a secure, out-of-band fashion to effect certificate issuance.

When a CA key rollover is accomplished, the GPO-CA shall issue a key rollover certificate, which the COTS PKI software shall automatically make available in the GPO border directory. The trust anchor certificate shall be provided to Subscribers on a CD at the time of Subcriber in-person identity proofing.

6.1.5 Key Sizes

The GPO-CA use of Secure Socket Layer (SSL), or TLS, or another protocol providing similar security to accomplish any of the requirements of this CP, if any, shall require at a minimum Triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys. When the GPO-CA uses SSL or TLS or any other similar security protocol, Triple DES or stronger shall be used for the symmetric key, and at least 1024 bit RSA or equivalent for asymmetric keys. After 12/31/08, the GPO-CA shall use AES (128 bits) or equivalent for the symmetric key, and shall use 2048 bit RSA or equivalent for the asymmetric keys.

The GPO-CA key modulus shall be a minimum of 2048 bits for RSA.

The GPO-CA CSS system key modulus shall be a minimum of 2048 bits for RSA.

Subscriber’s key modulus shall be 2048 bits for RSA.

The GPO-CA shall use Triple DES or AES-256 for database encryption.

Certificates issued under this CP, including CSS certificates, shall use the following OIDs for signatures:

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha-256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Certificates under this CP will use the following OIDs for identifying the algorithm for which the subject key was generated:

RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186.

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186 or a more stringent test if specified by the GPO-PA.

6.1.7 Key Usage Purposes (as Per X.509 v3 Key Usage Field)

Keys are certified for use in signing, non-repudiation or encrypting. Public keys that are bound to human subscribers shall be used only for signing or encrypting, but not both. Subscriber certificates used for digital signatures (including authentication) will set the *digitalSignature* bit and the *nonRepudiation* bit (except for Device certificates). Device certificates issued will not have the *nonRepudiation* bit set. Certificates to be used for key or data encryption shall set the *keyEncipherment* and/or the *dataEncipherment* bit. GPO-CA certificates shall set two key usage bits: *cRLSign* and *CertSign*. Certificates to be used for key agreement, if used by the GPO-CA, shall set the *keyAgreement* bit.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* the latest version of FIPS 140 series. The GPO-PA may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the GPO-PA. Cryptographic modules shall be validated to the latest version of the FIPS 140 series level identified in this section. The minimum FIPS 140 requirements for cryptographic modules are as follows:

- Certification Authority (CA) - Level 3 Hardware
- CSS – Level 2 Hardware
- Subscriber:
  - Level 1 Hardware or Software for GPO Medium Assurance, GPO Device, fpki-common-device and fpki-common certificates
  - Level 2 Hardware for GPO Medium-Hardware Assurance, fpki-common-hardware, fpki-common-authentication, fpki-common-cardAuth, GPO Authentication and GPO CardAuth certificates
- Registration Authority (RA) - Level 2 Hardware

Private key storage for GPO-CA Subscribers that assert the GPO Medium Hardware OID for id-gpo-medium-hardware shall use a FIPS 140 Level 2 or higher validated cryptographic module for all private key operations.

6.2.2 GPO-CA Private Key (n out of m) Multi-Person Control

Use of the GPO-CA private signing key shall require action by multiple persons as set forth in Section 5. of this CP.

6.2.3 Private Key Escrow

Under no circumstances shall the GPO-CA signature keys used to support non-repudiation services be escrowed by a third-party.

6.2.3.1 Escrow of CA Encryption Keys

The GPO-CA shall not perform any encryption key recovery functions involving encryption keys issued to Entity CAs.

6.2.4 Private Key Backup

6.2.4.1 Backup of GPO-CA Private Signature Key

The GPO-CA private signature keys shall be backed up under the same multi-person control as the creation of the original signature key. Such backup shall create only a single copy of the signature key at the GPO-CA location; a second copy may be kept at the GPO-CA backup location. Procedures for this shall be included in the GPO CPS.

6.2.4.2 Backup of Subscriber Private Signature Key

Subscriber private signature keys shall not be backed up, escrowed, copied or archived.

6.2.4.3 Backup of Subscriber Private Key Management Key

Backed up Subscriber private key management key shall not be stored in plaintext outside of the cryptographic module.

6.2.4.4 Backup of CSS Private Key

The CSS Private Key may be backed up. The backup process shall be secure and utilize the same level of protection as for the original CSS private key.

6.2.5 Private Key Archival

Private signature keys shall not be backed up, escrowed, or copied.

The CA private signature key shall not be archived. The CA private signature key shall be stored inside a FIPS compliant hardware token (compliant to FIPS 140 at Security Level 3) and no backup CA key storage tokens shall ever be sent to the secure archive facility.

Subscriber private signature keys shall not backed up, escrowed, copied or archived.

The GPO-CA shall use FIPS certified COTS CA software to escrow key management keys for Subscribers to enable key recovery, and the protocols and cryptographic methods of the FIPS certified COTS CA software shall be used for this purpose. COTS CA software that meets FIPS standards and requirements shall use cryptographic parameters, including Triple DES or AES-256 symmetric key encryption for CA database encryption, which are as strong or stronger than the key management keys being protected.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

GPO-CA private keys shall be generated by and remain in a cryptographic module. The GPO-CA private keys may be backed up in accordance with Section 6.2.4.1.

6.2.7 Private Key Storage on a Cryptographic Module

FIPS 140 requirements and section 6.2.1 above of this CP define the requirements.

6.2.8 Method of Activating Private Keys

The subscriber must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9 Method of Deactivating Private Key

If cryptographic modules are used to store private keys, then the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable GPO CPS. Hardware cryptographic modules shall be removed and stored in a secure container when not in use and not in the possession of the private key owner.

6.2.10 Method of Destroying Private Key

When the CA private key is to be destroyed, this shall only be under the conditions that the key is no longer needed and the certificates which correspond to it are expired or revoked, then this shall be performed using the FIPS compliant hardware module's zeroize command in accordance with the hardware module vendor's documentation. This shall be a scripted event with a written script, and only Trusted Role staff may perform this operation. The command shall be repeated at least one (1) time to ensure that the private key is destroyed. The applicable FIPS compliant hardware module shall be retained in storage at the GPO PKI facility, secured in a GSA compliant security container, in this event.

For Subscriber private keys that are stored on a hardware token, the vendor supplied software command to re-initialize and zeroize the token shall be used, following the documentation of the vendor.

6.2.11 Cryptograhic Module Rating

See section 6.2.1 for this information.

6.3 Other Aspects of Key-Pair Management

A subscriber's key-pair that is used for digital signatures shall never be escrowed, archived or backed up, because a subscriber can repudiate a transaction if there is a copy of his or her digital signature private key in existence.

For information that is encrypted, the subscriber shall use his or her private encryption (confidentiality) key to decrypt the information. If that private key is lost or destroyed, or if the subscriber departs GPO without relinquishing the private key, or acts maliciously, there is no way to decrypt the information. Thus, for business continuity reasons, GPO must be able to escrow, backup or archive private keys used for decrypting files and e-mails, while not escrowing, backing up or archiving key-pairs used for authentication. This means that two separate key pairs need to be employed.

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Certificate Operational Periods and Key Usage Periods

The GPO-CA, since it employs a self-signed certificate for use as a trust anchor, shall limit the use of the associated private key to a maximum of 20 years; the self-signed certificate shall have a lifetime not to exceed 37 years. For all other CAs under this CP, the CA shall limit the use of its private keys to a maximum of four years for subscriber certificates and ten years for CRL signing and OCSP responder certificates. Code and content signers may use their private keys for three years; the lifetime of the associated public keys shall not exceed eight years. Subscribers' signature private keys and certificates have a maximum lifetime of three years. Subscriber key management certificates have a maximum lifetime of 3 years; use of subscriber key management private keys is unrestricted.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data used to unlock GPO-CA or subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. Activation data may be user selected. Activation data shall be generated in conformance with FIPS 112. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic

module. When CA re-key occurs, any passwords used by the GPO-CA as activation data for the CA signing key shall be changed.

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should either be biometric in nature or memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. The protection mechanism shall include a facility to temporarily lock the account, or terminate the application after a predetermined number of login attempts as set forth in the GPO-CA CPS.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The GPO-CA and its components shall include the following functionality:

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Restrict access control to GPO-CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object re-use or require separation for GPO-CA random access memory
- Require use of cryptography for session communication and database security
- Archive GPO-CA history and audit data
- Require self-test security related GPO-CA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanisms for keys and the GPO-CA system
- Enforce domain integrity boundaries for security critical processes

When GPO-CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration..

6.5.2 Computer Security Rating

No Stipulation.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

The System Development Controls for the GPO-CA are as follows:

- The GPO-CA shall use software that has been designed and developed under a development methodology
- The GPO-CA shall use COTS CA software that meets FIPS requirements.
- Hardware and software procured to operate the GPO-CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with
- Hardware and software developed specifically for the GPO-CA shall be developed in a controlled environment, and the development process shall be defined and documented (this requirement does not apply to commercial off-the-shelf hardware or software)
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the GPO-CA physical location
- The GPO-CA hardware and software shall be dedicated to performing one task: the GPO-CA. There shall be no other applications, hardware devices, network connections, or component software, which are not part of the GPO-CA operation
- Proper care shall be taken to prevent malicious software from being loaded onto the GPO-CA equipment. Only applications required to perform the operation of the GPO-CA shall be obtained, from sources authorized by local policy. RA hardware and software shall be scanned for malicious code on first use and periodically afterward
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the GPO-CA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the GPO-CA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the GPO-CA system. The GPO-CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

The Principal (root) GPO-CA shall not be connected to any network. The Subordinate GPO-CA shall be connected to at most one network. Use of appropriate boundary controls shall be employed, such as network guards, firewalls or filtering routers to guard against denial of service and intrusion attacks. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the GPO-CA.

The GPO-CA CPS shall define the network protocols and mechanisms required for the operation of the GPO-CA Border Directory. Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 TIME-STAMPING

Asserted times shall be accurate within three (3) minutes. Use of automated methods via a NIST clock source and the Network Time Protocol (NTP) service is allowed as are manual methods. Clock adjustments are an auditable event per section 5.4.1 of this CP.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

The GPO-CA issues X.509 Version 3 certificates and shall support the following fields:

A. Version: Version field is set to v3.

B. Signature: Identifier for the algorithm used by the GPO-CA to sign the certificate. ; Algorithm identifier (RSA with SHA-1 (for certificates that expire on or before December 31, 2010) or RSA with SHA-256 (for certificates that expire on or after January 1, 2011).

C. Issuer: Certificate issuer (CA) Distinguished Name

D. Validity: Certificate validity period - notBefore start date and notAfter end date are specified

E. Subject: Certificate subject Distinguished Name

F. Subject public key information: Algorithm identifier (RSA or DSA with SHA-1), and public key

The CPS shall define in detail the actual format of certificates issued by the GPO-CA.

Certificates issued by the GPO-CA shall conform to the Federal PKI (FPKI) X.509 Certificate and CRL Extensions Profile (CCP-PROF).

7.1.1 Version Number(s)

The GPO-CA shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CAs and communities. Certificates shall use *the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the US Federal PKI Shared Service Providers (SSP) Program e* [CCP-PROF]. Whenever private extensions are used, they shall be identified in a CPS. Critical private extensions shall not be used in GPO-CA certificates. Critical private extensions may only be used in Subscriber certificates, and if used, shall be interoperable in their intended community of use.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha-256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Certificates under this CP shall use the following OIDs for identifying the algorithm for which the subject key was generated:

RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}

7.1.4 Name Forms

Where required as set forth above, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC3280.

7.1.5 Name Constraints

The GPO-CA shall assert name constraints in certificates it issues.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP shall assert the OID appropriate to the level of assurance with which it was issued.

7.1.7 Usage of Policy Constraints Extension

The GPO-CA may optionally assert policy constraints in CA certificates. This shall be documented and specified in detail in the CPS, if it is employed.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical certificate policy extension used by the GPO-CA shall conform to the Federal Certificate Profile issued by NIST.

7.2 CRL PROFILE

7.2.1 Version Number(s)

The GPO-CA shall issue X.509 version two (2) CARLs/CRLs.

7.2.2 CARL and CRL Entry Extensions

Detailed CARL/CRL profiles addressing the use of each extension shall conform to the Federal Certificate Profile issued by NIST.

7.3 OCSP PROFILE

Certificate Status Servers operating under this CP shall sign responses using algorithms designated for CRL signing.

The CSS shall be able to process SHA-1 hash values if they are included in the CertID field and the KeyHash in the responder ID field, and the CSS for the GPO-CA shall be configured for this.

7.3.1 Version Number(s)

The GPO-CA shall issue Version 1 OCSP certificates.

7.3.2 OCSP Extensions

There shall be no critical OCSP extensions in the OCSP Profile issued by the GPO-CA. Detailed OCSP profiles addressing the use of each extension shall conform to the CCP-PROF profile.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

CAs shall have a compliance audit mechanism in place to ensure that the requirements of the GPO CP are being implemented and enforced.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The GPO CAs (including CSS components) and RAs shall be subject to a periodic compliance audit/assessment which is no less frequent than once per year.

The GPO-CA has the right to require periodic and aperiodic compliance audits or inspections of CA or RA operations to validate that the entities are operating in accordance with the security practices and procedures described in their respective CPS. Further, the GPO-PA has the right to require aperiodic compliance audits of CAs. The GPO-PA shall state the reason for any aperiodic compliance audit.

Assessments shall take place upon on the initial activation of a new CA (a brand new CA or new DN for a CA) and once every 12 months thereafter in accordance with federal PKI Common Policy and GPO CP requirements.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The assessor or compliance auditor must perform PKI compliance audits as a regular ongoing business activity. The auditor must be a certified information system auditor (CISA) or IT security specialist (such as a certified information systems security professional or CISSP), and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

The GPO PA will have the responsibility to verify that the assessor or compliance auditor selected, by the GPO-OA, to audit the GPO PCA and any applicable personnel meet the requirements governing the identity and qualifications of the assessor/compliance auditor that are stipulated in this CP.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor or assessor is a firm in a contractual relationship with the GPO and has no GPO PKI management capabilities or responsibilities.

8.4 TOPICS COVERED BY ASSESSMENT

The compliance audit verifies that the operational and technical controls used by the GPO-CA operations personnel, including all RA's, satisfy all requirements of this CP and the Federal PKI Common Policy, as well as any MOA's between the GPO-CA and any other PKI or entity, including all the following topics:

- Identification & Authentication
- Certificate Life-Cycle Operational Requirements
- Facility, Management, and Operational Controls
- Technical Security Controls
- Certificate, CRL and OCSP Profiles
- CPS Administration

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the compliance auditor finds a discrepancy between how the GPO-CA is designed or is operated or maintained, as compared to the requirements of the GPO CP and/or Federal PKI CP, or with any MOA's or applicable CPS, the following actions shall be performed:

- the compliance auditor shall document the discrepancy

- the compliance auditor shall notify the GPO PKI PA and Operational Authority promptly

- The GPO PKI PA and OA shall promptly determine what further actions are necessary to meet the requirements of the GPO CP, Federal PKI CP, GPO-CA CPS, and any relevant MOA's. The GPO PKI PA and OA shall make any such required notifications and take such actions without delay.

Relevant to bullet item #3 above, there are three possible additional actions to take when a deficiency has been identified by the compliance auditor:

- Continue to operate as usual
- Continue to operate but at a lower assurance level
- Suspend operation

If a deficiency is identified, the GPO PA will determine which of the following actions to take.

- If continuing operation, as usual or lower assurance level, the GPO PA and OA are responsible for ensuring that corrective actions are taken within 30 days. At that time, or earlier if agreed by the GPO PA and Compliance Auditor, the compliance audit team will re-audit the GPO PCA in the areas of deficiencies. If, upon re-audit, corrective actions have not been taken, the GPO PA will determine if more severe action is required.

- If operation is suspended the GPO PA and OA are responsible for reporting the status of corrective action to the Compliance Auditors on a weekly basis. The GPO PA and Compliance Auditor together will determine when re-audit is to occur. If the deficiencies are deemed to have been corrected upon re-audit, the GPO PCA will resume service.

8.6 COMMUNICATION OF RESULT

The compliance auditor will communicate results of all compliance audits to the GPO PA through a Compliance Audit Report letter. This report letter shall document the versions of the CP and CPS used in the compliance audit. A copy of this report letter shall be communicated by the GPO PA to the federal PKI PA. Additionally, where necessary, the results of the compliance audit shall be communicated by the GPO PA as described in section 8.5 above.

. A special compliance audit shall be conducted if it is required to confirm the implementation and effectiveness of the remedy to any deficiencies documented by the compliance auditor. The federal PKI Policy Authority can determine that such a special compliance audit is required to verify implementation and effectiveness of the remedy, and the GPO PA can do so as well.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

GPO may charge fees for certificate issuance and renewal and these fees shall be set by GPO and documented with Subscribers.

9.1.2 Certificate Access Fees

There are no charges for access to the GPO-CA certificate or to Subscriber certificates.

9.1.3 Revocation or Status Information Access Fees

There are no charges for access to Revocation, CRL or CSS Status information.

9.1.4 Fees for Other Services

GPO reserves the right to set fees in accordance with this CP and MOA's for other services provided by the GPO-CA.

9.1.5 Refund Policy

Refunds are subject to a case by case review by the GPO PA and the Subscriber's organization.

9.2 FINANCIAL RESPONSIBILITY

Organizations that are acting as Relying Parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction. Acceptance of a Medium Assurance or Medium-Hardware Assurance Level certificate is entirely at the discretion of the organization acting as a Relying Party and is likely to depend upon several factors such as, the likelihood of fraud, other procedural controls, organization-specific policy, or statutorily imposed constraints.

9.2.1 Insurance Coverage

There shall be no insurance coverage for any non-GPO entity or external party, or any Relying Party.

9.2.2 Other Assests

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

There is no insurance coverage or warranty coverage of any kind for end-entities or for relying parties offered by the GPO-CA.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

GPO-CA information not requiring protection may be made publicly available, subject to the stipulations of this CP and the federal PKI Common Policy, and any applicable MOA.

9.3.1 Scope of Confidential Information

Each Subscriber's private signing key is confidential to that Subscriber. The CA and RA are not provided any access to those keys.

Information held in audit logs and the archives is considered confidential to the GPO-CA and is not released to external parties, unless required by law.

Personal information held by the RA, other than that which is explicitly published as part of a certificate, CRL, this CP or the CPS is considered confidential to the GPO PKI and is not released unless required by law.

. Information stored on the RA workstation or GPO-CA server is protected by password. The RA keeps paper information (e.g., registration forms) in a locked container when the RA is not present.

9.3.2 Information not within the Scope of Confidential Information

Information included in certificates and CRLs issued by the GPO-CA are not considered confidential, with the exception of the FASC-N value in the subject alternative name extension in all GPO Authentication certificates.

9.3.3 Responsibility to Protect Confidential Information

The GPO-CA PA and OA shall have responsibility to ensure that controls exist to protect the confidential information in section 9.3.1.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

A Privacy Impact Assessment (PIA) for the GPO-CA shall be produced by GPO and shall involve the GPO Privacy Officer. The PIA shall be made available to the compliance auditor and the Federal PKI Policy Authority. If deemed necessary by the GPO PA, a Privacy Plan shall be produced and implemented in accordance with GPO policies.

9.4.2 Information Treated as Private

Information held in the GPO-CA audit logs and the GPO-CA archives is considered private and shall not released to external parties (with the exception of the Federal PKI Policy Authority), unless required by law.

9.4.3 Information Not Deemed Private

Information included in certificates and CRLs issued by the GPO-CA are not considered confidential, with the exception of the FASC-N value in the subject alternative name extension in all common-authentication (PIV Authentication) and GPO Authentication certificates.

9.4.4 Responsibility to Protect Private Information

The GPO-CA PA and OA shall have responsibility to ensure that controls are in force and operational to securely store and protect the private information discussed in section 9.4.

9.4.5 Notice and Consent to Use Private Information

There are no requirements for the GPO-CA to provide notice or obtain consent to use the information provided by Subscribers and applicants for certificates.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The GPO PA is the responsible party to review all requests for information release as part of civil discovery and, working with the GPO Policy Authority, GPO General Counsel and Federal PKI Policy Authority shall ensure that no private information or GPO-CA information is disclosed unless required by US federal law or ordered by a court with valid jurisdiction.

The GPO PA keeps copies, either paper or electronic, of each request for information release pursuant to judicial or administrative process, and to law enforcement officials.

9.4.7 Other Information Disclosure Circumstances

None.

9.5 Intellectual Property Rights

The GPO PA and OA shall comply with intellectual property rights.

All Certificates and CRLs issued by the GPO-CA are the property of the GPO-CA. This CP is the property of the GPO-CA. The Distinguished Names (DNs) for GPO entities within the GPO-CA domain in the directory and in certificates issued to GPO entities within that domain are the property of GPO. The DNs for non-GPO entities are subject to the MOA between the entity and GPO.

With respect to licensed applications, this CP does not modify ownership of licensed applications or licensing agreements for such applications.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The GPO-CA who issues certificates that assert this policy shall comply with the stipulations of the US Federal PKI Common Policy and will comply with the requirements set forth in any MOAs that may be appropriately executed. The GPO-CA shall make GPO certificates and CRLs available in a repository for subscribers, PKI administrators and Relying Parties use.

The GPO-CA does not disclaim any responsibilities required under the Federal PKI Common Policy Framework.

The GPO-CA may use a variety of mechanisms for posting information into a repository as required by the US Federal PKI Common Policy and this CP. These mechanisms at a minimum shall include:

- All CA certificates and CRL's shall be placed into a X.500 Directory Server System that is publicly accessible through the Lightweight Directory Access Protocol (LDAP)

- All CA certificates and CRL's shall also be available and publicly accessible via the Hyper Text Transport Protocol (HTTP)
- The GPO-CA may optionally publish subscriber certificates into the publicly accessible X.500 Directory Server System that is publicly accessible through LDAP protocol
- Availability of the information as required by the certificate information posting and retrieval stipulations of the US Federal PKI Common Policy and the GPO CP
- Access control mechanisms when needed to protect repository information from unauthorized modification or deletion (as described in later sections)
- There shall be redundant directory systems (a total of 3 directory systems for triple redundancy) at the primary operational site and in addition, redundant directory systems at the off-site backup operational site (a total of 3 directory systems for triple redundancy at the off-site backup location) so that the GPO-CA can achieve the Common Policy directory availability requirements.
- The publicly accessible directory systems and LDAP and HTTP access mechanisms shall be operated and maintained to comply with the Federal PKI Common Policy Framework requirements for overall availability, and the scheduled downtime for these systems will be limited to ensure that Federal PKI Common Policy Framework requirements are met at all times
    - The schedule downtime requirements in the Federal PKI Common Policy are met by tracking all scheduled downtime in GPO PKI Change Control Records and ensuring that one of the redundant systems is always planned to be online and active, to avoid any downtime while other redundant systems might undergo scheduled maintenance or problem resolution.

9.6.2 RA Representations and Warranties

The RA will abide by all obligations and all stipulations defined in the US Federal PKI Common Policy for Common-Policy, Common-Authentication, Common-Hardware, Common-cardAuth, and Common-Device certificates, for all GPO CP obligations, and shall also abide by this CP. The RA shall ensure that the cryptographic module shall not left unattended once the private key is activated, in order to ensure that unauthorized access to the private key does not occur.

RA's shall conform to the stipulations of the Federal PKI Common Policy and this CP including:

- Maintaining RA operations in conformance with this CP
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate

- Ensuring that obligations are imposed on Subscribers via the Subscriber Agreement, and that Subscribers are informed of the consequences of not complying with the obligations contained in the Subscriber Agreement and this CP (by informing Subscribers that their certificate can be revoked for non-compliance with the Subscriber Agreement and this CP).

RA's that are found to have acted in a manner inconsistent with these obligations in this CP or the Federal PKI Common Policy shall be subject to revocation of RA responsibilities.

9.6.3 Subscriber Representations and Warranties

Subscriber obligations are specified in the Subscriber agreement, including requirements for protecting the private key and use of the certificate,that each Subscriber applicant must sign prior to the time they receive their keys and certificates. This agreement includes an obligation that the cryptographic module shall not be left unattended by the Subscriber once the private key is activated. These requirements apply to human sponsors associated with Device certificates issued under id-fpki-common-devices.

9.6.4 Relying Parties Representations and Warranties

This CP (as well as the US federal Common Policy) does not specify what steps a Relying Party should take to determine whether to rely upon a certificate. The Relying Party decides, pursuant to its own policies, what steps to take. The GPO-CA provides the tools needed to perform the trust path creation, validation, and certificate policy mappings which the Relying Party may wish to employ in its determination. The GPO-CA shall make GPO certificates and CRL's available in a repository and shall also make certificate status available via OCSP so that Relying Parties may obtain GPO certificates and CRL's for Relying Party use (pursuant to Relying Party policies).

The Relying Party must determine if the certificates issued under the GPO-CA are appropriate for their application. This may be determined by evaluating various risk factors including the value of the information, the threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by the GPO-PA or the GPO-OA.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

The GPO-CA does not disclaim any responsibilities required by the federal PKI Common Policy or the GPO Certificate Policy.

9.8 LIMITATIONS OF LIABILITY

The GPO shall not liable to any party with respect to the operations of the GPO-CA except in accordance with federal law, or through a valid express written contract between GPO and another party.

In no event will the GPO be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by or revoked by, or not revoked by, the GPO-CA.

Certificates are issued and revoked at the sole discretion of the GPO-PA. When the GPO-CA issues a cross-certificate, it does so for the convenience of the GPO and in compliance with the provisions of the US federal PKI Common Policy and the GPO CP. The Entity must determine whether the US Federal PKI Common Policy or the GPO CP meets its legal and policy requirements. Review of an Entity's CP by the GPO is not a substitute for due care and mapping of the CP by the Entity, including Relying Parties.

9.9 INDEMNITIES

No stipulation.

9.10 TERM AND TERMINATION

9.10.1 Term

This CP becomes effective when approved by the GPO PA and OA. There is no specified term for this CP.

9.10.2 Termination

Termination of this CP is at the discretion of the GPO PA. The Federal PKI Policy Authority shall be notified by email and telephone if this CP is terminated.

9.10.3 Effect of Termination and Survival

The effects of this CP apply until the end of the archive period of the last certificate issued by the GPO-CA.

9.11 Individual Notices and Communication with Participants

The GPO PA shall notify and communicate with participants via instructions and methods contained in MOA's.

9.12 Amendments

9.12.1 Procedure for Amendment

The GPO PA shall review this CP at least annually. Corrections or changes to this CP shall be made available to all Subscribers and Participants, via publication of the CP on the Internet at the GPO PKI web site (http://www.gpo.gov/projects/pki.htm).

Suggested changes to this CP may be provided to the Contact Person listed in section 1.5.2 of this CP. Such suggested change must include a description of the change, a justification for why the change should be implemented and contact information for the requestor.

9.12.2 Notification Mechanism and Period

Changes to this CP shall be communicated to the Federal PKI Policy Authority (FPKIPA) in accordance with the MOA between the GPO and the FPKIPA. In addition, changes to this CP shall be communicated to all non-GPO agencies that have an MOA in effect with the GPO PA via electronic mail (email) to the contact person listed in the MOA.

9.12.3 Circumstances under which OID must be Changed

An OID will be changed if the GPO PA or FPKIPA determine that the assurance level of the certificates do not meet the applicable GPO CP or Federal PKI Common Policy.

9.13 Dispute Resolution Provisions

The GPO-PA shall resolve any disputes associated with the use of the GPO-CA or certificates issued by the GPO-CA.

9.14 Governing Law

The terms and provisions of this CP shall be interpreted under and governed by applicable Federal law.

9.15 Compliance with Governing Law

The GPO PKI, PA, OA and this CP shall comply with federal law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should it be determined that any relevant section of this Certificate Policy is incorrect or invalid, all other parts of the CP shall remain in effect until such time as the CP can be updated. The process for updating the CP is described in section of 9.12 of this CP.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 OTHER PROVISIONS

No stipulation.

10. BIBLIOGRAPHY

The following documents were used in part to develop this CP:

ABADSG	Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html
CCP-PROF	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program. http://www.cio.gov/fpkipa/documents/CertCRLprofileForCP.pdf
FIPS 112	Password Usage, 1985-05-30 http://csrs.nist.gov/
FIPS 140-1	Security Requirements for Cryptographic Modules, 1994-01 http://csrs.nist.gov/fips/fips1401.htm
FIPS 140-2	Security Requirements for Cryptographic Modules, 2001-06 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 180-1	Secure Hash Standard, 1995-04 http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf
FIPS 180-2	Secure Hash Standard, 2002-08 http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf
FIPS 186	Digital Signature Standard, 1994-05-19 http://csrs.nist.gov/fips/fips186.pdf
FIPS 186-2	Digital Signature Standard, 2000-01 http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
FOIACT	5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997. ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. http://www4.law.cornell.edu/uscode/40/1452.html
NAG69C	Information System Security Policy and Certification Practices Statement for Certification Authorities, rev C, November 1999.
NSD42	National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)
NS4005	NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.

NS4009 NSTISSI 4009, National Information Systems Security Glossary, January 1999.

PKCS#12 Personal Information Exchange Syntax Standard, April 1997.
http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html

RFC 2510 Certificate Management Protocol, Adams and Farrell, March 1999.

RFC 2527 Certificate Policy and Certificate Practices Framework, Chokhani and Ford, March 1999.

Security Requirements for Certificate Issuing and Management Components, 3 November 1999, Draft

Digital Signatures, W. Ford

United States Department of Defense X.509 Certificate Policy, Version 5.0, 13 December 1999

11. ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
CARL	Certificate Authority Revocation List
COMSEC	Communications Security
COTS	Commercial Off-the-Shelf
CP	Certificate Policy
CCP-PROF	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the US Federal PKI Shared Service Providers (SSP) Program.
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FBCA Operational Authority	Federal Bridge Certification Authority Operational Authority
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKISC	Federal PKI Steering Committee

FPKIPA	Federal PKI Policy Authority
GPEA	Government Paperwork Elimination Act of 1998
GPO-CA	Government Printing Office Certification Authority
GPO-CA Operational Authority	Government Printing Office Certification Authority Operational Authority
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
MOA	Memorandum of Agreement (as used in the context of this CP, between an Entity and the GPO-PA allowing interoperation between the GPO-CA and Entity CA)
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments

RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TSDM	Trusted Software Development Methodology
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

12. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Agency CA	A CA that acts on behalf of an Agency, and is under the operational control of an Agency.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]

Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the Federal PKI Policy Authority or comparable Agency body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification

	authority issuing it. [ABADSG]. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certificate Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies it's Subscriber, (3) contains the Subscriber's public key, (4) identifies it's operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions,

	such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practices Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates that it has issued and that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Commercial Off-the-Shelf	A product, either hardware or software or both, that is a commercial product supported by a vendor in business for the purpose of selling and maintaining this product to service market commercial needs, including federal government needs.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.

Component Private Key	Private key associated with a function of the certificate issuing equipment, as opposed to being associated as opposed to being associated with an operator or administrator.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS140]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital

	certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate that is composed of two subfields: “date of issue” and “date of next issue”.
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Employee	Any person employed by an organization as defined above.
Encrypted Network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying Parties and Subscribers.
Entity	For purposes of this CP, Entity is any person, organization, corporation, or government (state, local, federal, or foreign) operating, or directing the operation of, one or more CAs.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity.

Federal Bridge Certification Authority (FBCA)	The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certification Practices Statements) that are used to provide peer-to-peer interoperability among Agency Principal Certification Authorities.
Federal Bridge Certification Authority Membrane	The Federal Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directory, Firewalls, Routers, Randomizers, etc.
FBCA Operational Authority	The Federal Bridge Certification Authority Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The Federal PKI Policy Authority is a federal government body responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the FBCA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Government Printing Office Certification Authority (GPO-CA)	The Government Printing Office Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certification Practices Statements) that are used to provide peer-to-peer interoperability among Other Certification Authorities.
GPO-CA Operational Authority	The Government Printing Office Certification Authority Operational Authority is the organization selected by the Government Printing Office Policy Authority to be responsible for operating the

	Government Printing Office Certification Authority.
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]

Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum of Agreement (MOA)	Agreement between the GPO PKI Policy Authority and an Entity allowing interoperability between the Entity CA and the GPO-CA.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related

	to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.

PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practices Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the Federal PKI Policy Authority.
Principal CA (PCA)	The Principal CA is a CA designated by an Agency to interoperate with the Entity CAs. An Agency may designate multiple Principal CAs to interoperate with the Entitiy CAs.
Privacy	Restricting access to subscriber or Relying Party information in accordance with Federal law and Organization policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.

Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Secret Key	A "shared secret" used in symmetric cryptography, wherein users are authenticated based on a password, Personal Identification Number (PIN), or other information shared between the user and the remote host or server. A single key is shared between two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated with an algorithm agreed to beforehand by the transacting parties.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA (SCA)	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA). Additionally, this CP may refer to CAs that are "subordinate" to the PCA. The use of this term shall encompass any CA under the control of the PCA that has a certificate issued to it by the PCA or any CA subordinate to the PCA, whether or not a hierarchical or other PKI architecture is used.
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device CAs are sometimes technically considered "subscribers" in a PKI.

	However, the term "Subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System High	The highest security level supported by an information system. [NS4009]
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Token	Hardware or software that contains or can be used to generate cryptographic keys. Examples of hardware tokens include smart cards and memory cards. Software tokens include both software cryptographic modules that store or generate keys and storage devices or messages that contain keys (e.g., PKCS #12 messages).
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.

Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS140]

13. ACKNOWLEDGEMENTS

The GPO PA, OA and authorized contractor support personnel developed this CP.